REMARKS

Claims 1-35 are pending in the application. It is gratefully acknowledged that Claims 1-11 and 20-29 have been allowed. It is also gratefully acknowledged that Claims 16-19, 34 and 35 have been objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form to include all of the limitations of the base claim and any intervening claims. The Examiner has rejected Claims 12-15, 30 and 31 under 35 U.S.C. §102(b) as being anticipated by Yatsukawa (U.S. Patent 6,148,404). The Examiner has rejected Claims 32 and 33 under 35 U.S.C. §103(a) as being obvious over Yatsukawa in view of Zhang et al. (U.S. Pub. 2002/0174335).

Please cancel Claims 32-35, without prejudice.

Regarding the rejection of independent Claims 12 and 30, the Examiner states that Yatsukawa anticipates the claims. Yatsukawa discloses enciphering a message by using a fixed (stored) secrete key Ks, so that seed data Ds_0 to be enciphered can be changed every time.

Claim 12 discloses a first private key generated from a secret previously shared with an authentication server and a second private key newly generated from first authentication information during next authentication, in which the first private key and the second private key are different from each other. On the contrary, Yatsukawa discloses using a secret key Ks stored in a Client X and enciphering a message by using the same secret key Ks during next authentication, so that only seed data to be enciphered can be changed.

Also, Claim 12 discloses enciphering a message with a first private key to be varied whenever authentication is performed, while Yatsukawa discloses enciphering a message by using a fixed (stored) secrete key Ks, so that seed data Ds_0 to be enciphered can be changed every time.

Further, Claim 12 discloses receiving a second enciphered message from the authentication server in response to the first enciphered message and acquiring a first session key, but Yatsukawa discloses that the Client X generates authentication data D1 by enciphering the first seed data using a client's secret key and sends the enciphered data to the server, and the server deciphers the received authentication data by using a public key K_p of the client to generate second inspection data, and compares the second inspection data with the first inspection data. In other words, Claim 12 discloses a method of acquiring a new key, while Yatsukawa discloses a method that only contents of the message to be enciphered are changed whenever the authentication is required, without changing a key value.

In conclusion, Claim 12 performs a secure communication between an access point (AP) and a mobile node by using the first session key, as discussed above. However, Yatsukawa merely discloses a method of granting an authentication request from a client to be logged in by determining whether Ds_0 obtained from a deciphering procedure coincides with Ds_0 read from a client-authentication data inspection data file.

Based on at least the foregoing, withdrawal of the rejection of Claim 12 is respectfully requested.

Regarding the rejection of dependent Claim 13 under §102(b) as being anticipated by Yatsukawa, Claim 13 recites, "the first authentication information includes a temporary identifier of the mobile node, a password for generating a private key to be used during next authentication, and a random number". The Examiner cites Yatsukawa at col. 16, lines 45-52, and Fig. 2 element "A1". First, element "A1" is merely a random number, not "a temporary identifier of the mobile node, a password for generating a private key to be used during next authentication, and a random number". Second, col. 16, lines 45-52 only disclose a user identification name, and not a temporary identifier of the mobile node; a user name is not a mobile node identifier. Even if these two elements could be seen as disclosed by Yatsukawa, which they are not, the Examiner does not cite any element that anticipates "a private key to be used during next authentication".

Based on at least the foregoing, withdrawal of the rejection of Claim 13 is respectfully requested.

Claim 30 recites, "receiving an enciphered message from the authentication server", and "acquiring a session key for secure communication with the mobile node by deciphering the enciphered message with a private key previously shared with the authentication server". The enciphered message, as used in Claim 30 and also as used in the specification and Claim 12, is generated from first authentication information. As argued above with respect to Claim 12, the first authentication information is unique to the present invention.

In Claim 30, when a mobile node hands over, a target AP to be accessed from a first AP to a second AP is changed, and when the mobile node tries to access, the second AP receives an enciphered message from an authentication server. Thus, it can be seen that the second AP is different from the first AP. In Yatsukawa, however, the authentication server to be logged into by clients is one in the same.

Further, Claim 30 discloses acquiring a session key by decoding the enciphered message using a private key previously shared with the authentication server for a secure communication between the AP and the mobile nodes. Meanwhile, Yatsukawa fails to disclose acquiring a new key like the session key as disclosed in the present invention.

Based on at least the foregoing, withdrawal of the rejection of Claim 30 is respectfully requested.

Regarding the rejection of dependent Claim 31 under §102(b) as being anticipated by Yatsukawa, Claim 31 recites "the enciphered message includes a temporary identifier generated by the mobile node during previous authentication, and a random number". Yatsukawa does not use previous authentication information in a one-time authentication process.

Based on at least the foregoing, withdrawal of the rejection of Claim 31 is respectfully requested.

Independent Claims 12 and 30 are believed to be in condition for allowance. Without conceding the patentability per se of dependent Claims 13-15 and 31, these are likewise believed to be allowable by virtue of their at least dependence on their respective amended independent claims. Accordingly, reconsideration and withdrawal of the rejections of dependent Claims 13-15 and 31 is respectfully requested.

Accordingly, all of the claims pending in the Application, namely, Claims 1-31, are believed to be in condition for allowance. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters, the Examiner may contact Applicants' attorney at the number given below.

Respectfully submitted,

Paul J. Farrell
Reg. No. 33,494
Attorney for Applicant

DILWORTH & BARRESE
333 Earle Ovington Blvd.
Uniondale, New York 11553
Tel: (516) 228-8484
Fax: (516) 228-8516

PJF/MJM/dr